Introduction à l'HIDS Wazuh

Introduction :

Wazuh est une plate-forme de sécurité gratuite et open source qui unifie les capacités d'un EDR/HIDS et SIEM. Il protège les infrastructures dans les environnements sur site, virtualisés, conteneurisés et basés sur le cloud.

Wazuh aide les organisations et les particuliers à protéger leurs actifs de données contre les menaces de sécurité. Il est largement utilisé par des milliers d'organisations dans le monde, des petites aux grandes entreprises.

I. Objectifs de la formation

Travaux en laboratoire permettant d'exploiter l'HIDS Wazuh afin d'aborder certaines compétences du bloc 3 sur la cybersécurité.

Dans ce cours nous verrons dans un premier temps comment installer l'environement de travail composé de du manager Wazuh, de 2 agents wazuh, un sur un système Linux et l'autre sur un système Windows. Par la suite nous verrons comment configurer Wazuh pour

Détecter les attaques suivantes :

- Détecter une attaque par force brute SSH
- Détecter une attaque par force brute RDP
- Exposer les processus caché (rootkit)
- Détecter les modifications du système de fichiers
- Détecter et réagir à une attaque Shellshock
- Surveillez l'exécution de commandes malveillantes
- Détectez le trafic réseau suspect
- Traquer les applications vulnérables

II. Les composants centraux de Wazuh

a. Serveur Wazuh

Le serveur Wazuh analyse les données reçues des agents Wazuh, déclenchant des alertes lorsque des menaces ou des anomalies sont détectées. Il est également utilisé pour gérer à distance la configuration des agents et surveiller leur état.

Le serveur Wazuh peut être installer sur un seul hôte. Il peut également être installer de façon distribuer sur plusieurs nœuds dans une configuration en cluster. Les configurations multi-nœuds offrent une haute disponibilité et des performances améliorées. Et s'il est combiné avec un équilibreur de charge réseau, une utilisation efficace de sa capacité peut être obtenue.

b. Wazuh indexer

L'indexeur Wazuh est un moteur de recherche et d'analyse en texte intégral hautement évolutif. Ce composant central Wazuh indexe et stocke les alertes générées par le serveur Wazuh et fournit des capacités de recherche et d'analyse de données en temps quasi réel.

c. Wazuh agent

L'agent Wazuh est multiplateforme et s'exécute sur les terminaux que l'utilisateur souhaite surveiller. Il communique avec le serveur Wazuh, envoyant des données en temps quasi réel via un canal chiffré et authentifié.

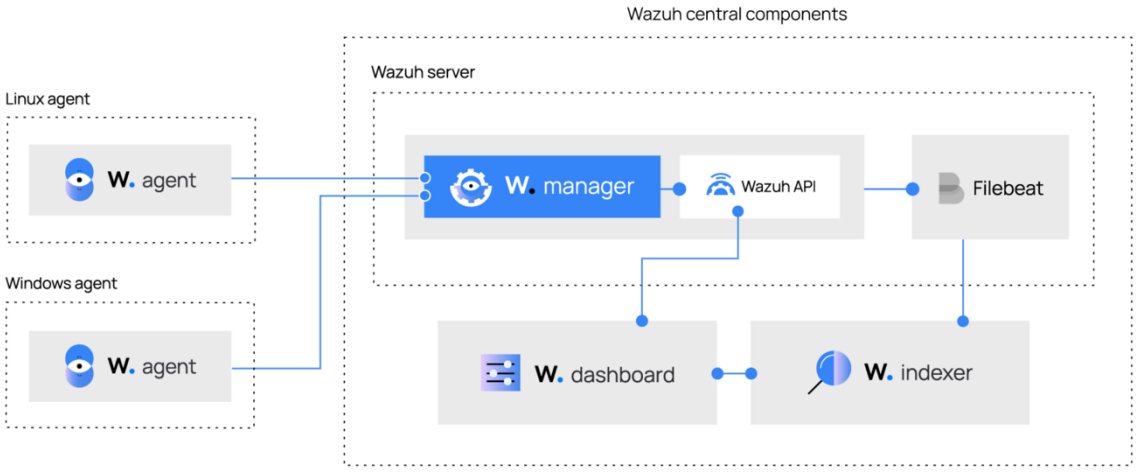
L'agent a été développé en tenant compte de la nécessité de surveiller une grande variété de terminaux différents sans affecter leurs performances. Il est pris en charge sur les systèmes d'exploitation les plus populaires et nécessite en moyenne 35 Mo de RAM.
L'agent Wazuh fournit des fonctionnalités clés pour améliorer la sécurité de votre système.

Collecteur de journaux	Exécution de commande
Surveillance de l'intégrité des fichiers (FIM)	Évaluation de la sécurité des configurations
Inventaire du système	Détection des logiciels malveillants
Réponse active	Sécurité des conteneurs
Sécurité du cloud	

III. Installation du laboratoire

Suivez ce TP pour configurer votre environnement de laboratoire. Tout d'abord, nous allons installer les composants centraux de Wazuh : le serveur Wazuh, l'indexeur Wazuh et le tableau de bord Wazuh.

L'infrastructure cible sera la suivante :



a. Installer les composants centraux Wazuh

Les composants centraux de Wazuh peuvent être installés sur un système d'exploitation Linux 64 bits, les systèmes d'exploitation recommandés sont :

- Red Hat Enterprise Linux 7, 8, 9
- CentOS 7, 8
- Ubuntu 16.04, 18.04, 20.04, 22.04

b. Installation du serveur Wazuh

Remarque : Pour exécuter toutes les commandes, les privilèges de l'utilisateur root sont requis.

1. Téléchargez et exécutez l'assistant d'installation de Wazuh.

```
curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh &&
sudo bash ./wazuh-install.sh -a
```

Une fois que l'assistant a terminé l'installation, la sortie affiche les informations d'identification d'accès et un message confirmant que l'installation a réussi.

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
    User: admin
    Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

Wazuh est maintenant installer et prêt à être configurer.

2. Accédez à l'interface web Wazuh avec https://<wazuh-dashboard-ip> et vos identifiants :

    - Nom d'utilisateur : administrateur
    - Mot de passe : <ADMIN_PASSWORD>

Lorsque vous accédez au tableau de bord Wazuh pour la première fois, le navigateur affiche un message d'avertissement indiquant que le certificat n'a pas été émis par une autorité de confiance. Ceci est normal et l'utilisateur a la possibilité d'accepter le certificat comme exception ou, alternativement, de configurer le système pour utiliser un certificat d'une autorité de confiance.

i. Configuration du serveur Wazuh

Configurer le gestionnaire Wazuh pour permettre l'auto-enregistrement des nouveaux agents avec authentification.

1. Exécutez les commandes suivantes pour activer l'authentification et définir le mot de passe pour l'enregistrement de l'agent.

```
# grep "<use_password>" -B7 -A8 /var/ossec/etc/ossec.conf
# sed -i 's/<use_password>no/<use_password>yes/'
/var/ossec/etc/ossec.conf
# grep "<use_password>" -B7 -A8 /var/ossec/etc/ossec.conf
# echo "please123" > /var/ossec/etc/authd.pass
```

Le mot de passe envoyé avec la commande echo dans /var/ossec/etc/authd.pass est celui que les agents utiliseront pour l'auto-enregistrement.

2. Redémarrez le gestionnaire Wazuh.

```
# systemctl restart wazuh-manager
```

3. Vérifiez que l'écouteur d'agent et l'écouteur d'auto-inscription sont en place :

```
# netstat -natp | egrep "(:1514|:1515)"
```

La sortie devrai ressembler à ceci :

```
tcp  0   0 0.0.0.0:1514  0.0.0.0:*  LISTEN  14311/wazuh-remoted
tcp  0   0 0.0.0.0:1515  0.0.0.0:*  LISTEN  14263/wazuh-authd
```

Installation de l'agent Wazuh sur un système Linux

Dans cette partie du TP nous allons utiliser cette procédure pour installer, enregistrer et configurer un agent Wazuh sur un système Linux.

Remarque : Pour exécuter toutes les commandes, les privilèges de l'utilisateur root sont requis.

Ajouter le référentiel Wazuh yum

```
# cat > /etc/yum.repos.d/wazuh.repo <<\EOF
[wazuh_repo]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=Wazuh repository
baseurl=https://packages.wazuh.com/4.x/yum/
protect=1
EOF
```

Installer et connecter l'agent Wazuh au manager

Créer la variable WAZUH_MANAGER pour qu'elle contienne l'adresse IP ou le nom d'hôte de votre gestionnaire Wazuh et exécutez la commande suivante pour installer et configurer votre agent Wazuh.

```
# WAZUH_MANAGER="<WAZUH_MANAGER_IP_ADDRESS>"
WAZUH_REGISTRATION_PASSWORD="please123" yum -y install wazuh-agent
```

Activez et démarrez le service d'agent Wazuh

```
# systemctl daemon-reload
# systemctl enable wazuh-agent
# systemctl start wazuh-agent
```

Vérifiez que l'agent s'est correctement connecté :

```
# grep ^status /var/ossec/var/run/wazuh-agentd.state
```

Vous devriez voir une sortie comme celle-ci :

```
# status='connected'
```

Remarque : Le fichier wazuh-agentd.state contient plusieurs informations utiles sur l'état de la connexion de l'agent Wazuh avec le gestionnaire Wazuh

Désactivez maintenant le référentiel Wazuh afin d'empêcher une future mise à jour involontaire qui pourrait provoquer un conflit de version avec l'installation actuelle.

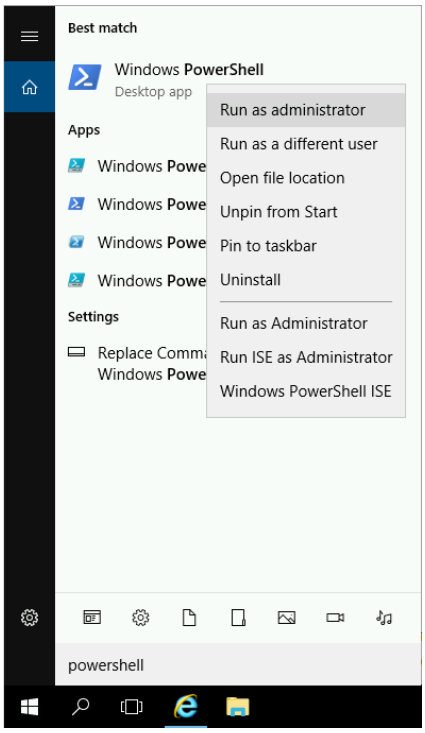
```
# sed -i "s/^enabled=1/enabled=0/" /etc/yum.repos.d/wazuh.repo
```

Installer l'agent Windows Wazuh

Dans cette partie du TP nous allons utiliser cette procédure pour installer, enregistrer et configurer un agent Wazuh sur un système Windows.

Remarque : Pour exécuter toutes les commandes, les privilèges de l'utilisateur root sont requis.

Cliquez sur l'icône **Search Windows** (loupe en bas à gauche de l'écran). Tapez : "PowerShell" et faites un clic droit sur Windows PowerShell.



Cliquez sur Exécuter en tant qu'administrateur.

Téléchargez et exécutez le programme d'installation avec la ligne de commande suivante. Assurez-vous de remplacer l'adresse IP dans `WAZUH_MANAGER` et `WAZUH_REGISTRATION_SERVER` par l'adresse IP ou le nom de domaine complet de votre gestionnaire Wazuh.

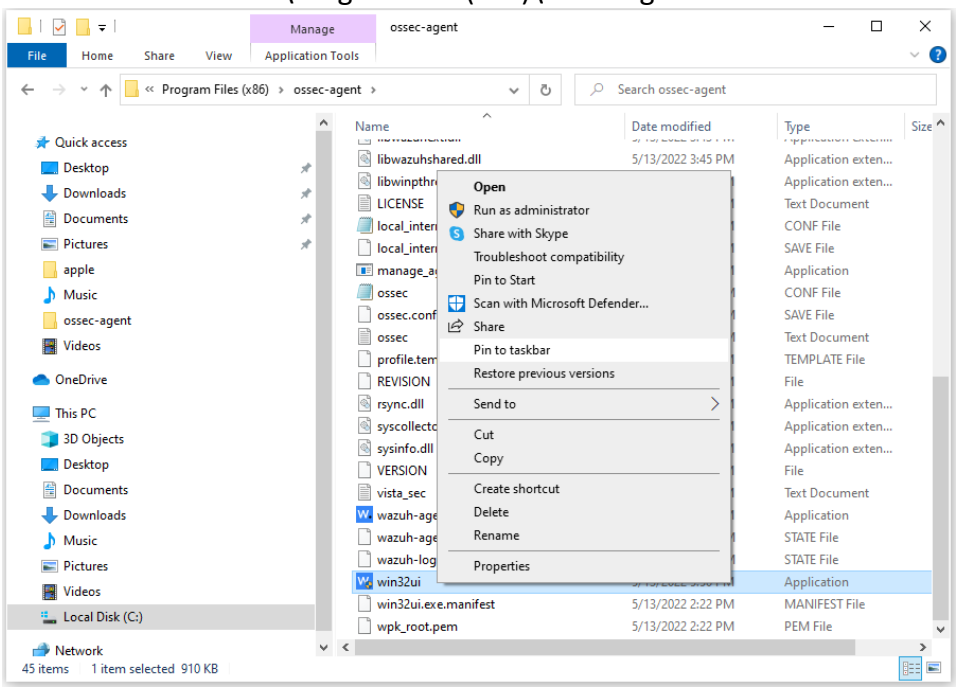
```
# Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.10-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.10.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.10.msi /q WAZUH_MANAGER='<WAZUH_MANAGER_IP_ADDRESS>' WAZUH_REGISTRATION_SERVER='<WAZUH_MANAGER_IP_ADDRESS>' WAZUH_REGISTRATION_PASSWORD='please123' WAZUH_AGENT_NAME="windows-agent"
```

Démarrez l'agent :

```
# NET START WazuhSvc
```

Créer un raccourci vers l'outil Wazuh agent Manager dans la barre des tâches :

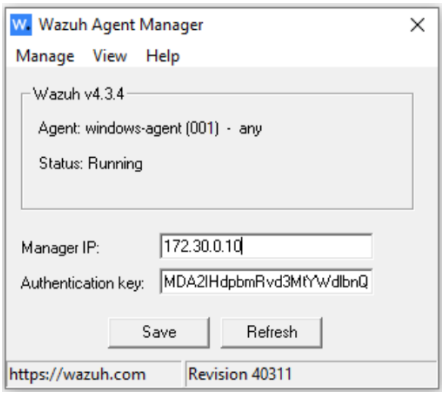
1. Ouvrez l'explorateur de fichiers (touche Windows + E).
2. Accédez au répertoire et recherchez l'exécutable **win32ui** .C:\Program files(x86)\ossec-agent



Cliquez avec le bouton droit sur le fichier win32ui et sélectionnez Épingler à la barre des tâches.

Exécutez le gestionnaire d'agent Wazuh et confirmez qu'il est en cours d'exécution et connecté au gestionnaire Wazuh.

1. Cliquez sur l'icône Wazuh dans votre barre des tâches. Ça devrait ressembler à ça:



En cliquant sur **Afficher** > **Afficher les journaux**, vous devriez trouver un enregistrement de l'agent ayant reçu avec succès une clé valide et se connectant au gestionnaire Wazuh.

En cliquant sur **Gérer**, vous pouvez **démarrer**, **arrêter** et **redémarrer** l'agent.

Sur le tableau de bord Wazuh, cliquez sur **Wazuh** > **Agents** pour passer en revue tous les agents enregistrés et leur statut.